PIN ADMINISTRATION POLICY

Association for Payment Clearing Services
Mercury House
Triton Court
14 Finsbury Square
LONDON
EC2A 1LQ

Telephone 020 7711 6200
Facsimile 020 7628 0924
Website www.apacs.org.uk

Produced for: **Card Payments Group**
Creation Date: **January 2004**

Version No.: **1.2**

Requests for such permission should be addressed to:

The Manager
Card Technology Section
APACS, Card Services
Mercury House
Triton Court
14 Finsbury Square
London
EC2A 1LQ

Any enquiries regarding the content of the document please email
david.baker@apacs.org.uk

TABLE OF CONTENTS

LIST OF FIGURES

DISTRIBUTION LIST

Card Payments Group	**CPG Smaller Issuers Community**	**Security Advisors Group**
Chip and PIN Forum	**Plastic Fraud Prevention Forum**	**Card Security Group**
Card Technology and Standards Group	**Acquirers' POS Group**	

DOCUMENT VERSION CONTROL:

Version	Author	Comment
0.2	A Chilver	First draft
0.4	A Chilver	Card Security Group Review Draft
0.51	C Whittaker & D Baker	APACS Draft following Card Security Group Review
0.52	C Whittaker	Draft for APACS Card Security Group approval and review prior to submission to the APACS Security Advisory Group and Card Technology and Standards Group.
0.6	C Whittaker & D Baker	Draft for Approval of Security Advisory Group
0.7	C Whittaker & D Baker	Draft for Approval of Card Technology and Standards Group
0.8	C Whittaker & D Baker	Incorporating comments following Card technology and Standards Group Review
0.9	C Whittaker & D Baker	Insertion of section on PIN Storage requirements.
1.0	C Whittaker & D Baker	Final version approved by Card Security Group for submission to Card Payment Group
1.1	C Whittaker & D Baker	Final version approved by Card Security Group for submission to Card Payments Group, incorporating LINK Pin management Service for reciprocal PIN change.
1.2	C Whittaker & D Baker	Final version for submission to Card Payments Group including comments from Chip and PIN Forum.

ABBREVIATIONS AND REFERENCES

Reference	Details	Synopsis
[FIPS_140]	FIPS 140 – Federal Information Processing Standard	
[ISO_8583]	ISO 8583 – Financial transaction card orientated messages- Interchange message specifications	
[ISO_9564]	ISO 9564 – Banking – Personal Identification Number Management and Security – Part 1: PIN protection principles and techniques	The banking industry international standard for PIN protection methodology.
[PED]	PIN Entry Device Protection Profile	

DEA1 Data Encryption Algorithm 1: same algorithm as DES

DEA2 Data Encryption Algorithm 2: same algorithm as RSA

DES Data Encryption Standard: Hardware implementation

ICC Integrated Circuit Card or Smart Card

MAC Message Authentication Code: integrity hash field

PAN Primary Account Number: frequently used to contain the card number

PIN Personal Identity Number

PEK PIN Encryption Key: used to protect PIN data in transit

PSK PIN Storage Key: used to protect reference PIN data in storage

PVV PIN Verification Value: used to form one-way encrypted PIN

RSA Public key algorithm due to Rivest, Shamir & Adelman

STIP Stand In Processing

1 Introduction

1.1 Objectives

APACS and its Members have initiated a UK-wide programme which is intended to transform the method of cardholder verification used in card payment transactions. This will introduce the need for customers to enter their PINs as part of the Cardholder Verification Method. This is known as the PIN @ POS programme. Currently, for non-ATM transactions, the identity of cardholders is verified by paper-based signatures. By 2005, it is planned to migrate to a PIN based verification method. One consequence of this programme will be a substantial expansion of the operational domain in which PINs will need to be used and managed. It is therefore appropriate to review the end-to-end process for the creation and management of PINs in the UK payments industry, with the following objectives:

- To define the PIN management process in terms of its life cycle and the components of that life cycle;
- To assign responsibility for each life cycle component between individual card issuers and the industry in general;
- To define industry policy for those components for which the industry is responsible; and
- To define recommended policies for those components for which individual card issuers are responsible.

1.2 Scope

This policy document has been developed following recommendations and instructions from the member financial institutions of the APACS Card Payments Group who will be implementing PIN @ POS Programme ('Members'), in order to:

- define the PIN management process in terms of its life cycle and the components of that life cycle; and
- achieve a consistent approach to PINs by all Members.

This policy document differentiates between "card issuer risk" and "industry risk". In general, industry risk is present where institutions are securing PIN assets that they do not necessarily own.

Consider the example of a card and PIN value issued by Bank A. Where that PIN value is handled in security domains owned and controlled by Bank A, this is deemed to be Bank A's risk and responsibility. Where the PIN is handled in security domains owned and controlled by other banks and institutions, this becomes an industry risk. Accordingly this policy document details:

- "Recommended Industry Positions" - Card issuers are responsible for PINs where the PIN value does not pass outside security domains controlled by it. Policies in areas owned by card issuers are normally presented in this document as "Recommended". It should be noted, however, that for reasons of industry reputation and brand protection, the imposition of Mandatory policies in this area is not excluded, although this is likely to be imposed through the payment schemes. These are positions that all of the Members consider to be best practice and necessary in order to provide a common customer experience in managing and using their PINs with their debit and credit cards. Recommended Industry Positions, in contrast to Mandatory Industry Positions, are at the discretion of the Members to implement.
- "Mandatory Industry Positions" – Where PINs pass through security domains controlled by multiple parties, a common industry position will be defined. Outside the auspices of APACS, Members have already committed to comply with a number of mandates imposed by bodies other than APACS. These include international standards, scheme-related security standards and agreed best practice. Members' submission to these mandates is entirely subject to the governance frameworks of those other bodies to which they have membership and is not impacted by this document. A number of those mandates - referred to here as Mandatory Industry Positions - are referenced for completeness, and are generally those required to be in place in order to achieve the level of interoperability required to facilitate reciprocal PIN change.

In approving this policy document Members agree that they will use it as an input to their own internal compliance processes. However, as each Member's technical and security architecture is unique, this policy document is not intended to be nor could it be an holistic guide to building a secure PIN administration architecture that is invulnerable to compromise. Each Member instead must review and determine the appropriateness of the Recommended Industry Positions contained, how best to implement them, and also what additional measures it should take in order to ensure a secure architecture.

1.3 Approach

The document was prepared following recommendations and instructions from the Members and provides the rationale for adopting policies and practices that have already been adopted by them. The following approach was taken in the preparation of this document:

- The Card Security Group agreed terms of reference for a study into PIN Administration Policy issues.
- A contractor was employed to conduct this study, during which industry views were sought. Sources included a cross section of card issuers and interested groups within the APACS structure, and Card and Interchange schemes.
- The PIN life cycle and its components are defined and this provides the organisational structure of this document.
- For each component, the relevant issues are identified.
- For each component, the industry policies are defined. These are derived, as appropriate, from:

- The views of APACS and its members;
- International standards; and
- Relevant views from the international security community.

1.4 Policy Maintenance

This policy statement will be updated and maintained by the APACS Card Security Group. In order to track probable changes to this document they will maintain an additional document providing the context and rationale of future issues that need to be reflected in this policy document. They will inform the Card Payments Group of the necessity for changes and updates to this policy statement, and use the context of such changes to generate Project Initiation Documents within their Work Plan to enable such changes to be made.

2 PIN Security Objectives And Architecture

2.1 Security Objectives

The following basic principles that should govern the PIN Management process are adapted from [ISO 9564]:

Assurance

It shall be possible to prove the security of the PIN Administration process.

The PIN Administration process must not only be secure, but also be demonstrably secure. If PIN Security is publicly challenged, either in the media or in a court of law, it must be possible to respond to such a challenge and for the response to be supported with evidence. Furthermore, the use of that evidence in the public domain must not in itself compromise security.

Cardinality

One PIN shall uniquely verify any one cardholder at any one time for a single transaction.

This does not preclude the use of more than one card product with different PINs, or the use of a single PIN to access multiple accounts.

Confidentiality

Plaintext PIN values and associated account details shall only be visible to cardholders. Card issuer personnel shall only handle plaintext PIN values where the associated account details are not available.

This principle protects card issuers from accusations that their personnel may be implicated in PIN security breaches. It recognises that plaintext PIN values can be handled by card issuer personnel provided that there is no reference to the account or customers to which the PIN is associated.

Design

The security of the PIN Administration process shall not rely on secrecy in the design.

This is a recognised security design principle that enables security design to be subjected to wide scrutiny.

Integrity

The integrity of the PIN shall be protected throughout its lifecycle.

For example, during personalisation when the PIN is loaded on the card, or alternatively when the PIN is transmitted in clear within an enclosed tamper resistant security domain.

2.2 Security Architecture And Life Cycle

"Figure 1: PIN Life Cycle" illustrates the collective set of functions in which a PIN participates during its life cycle.

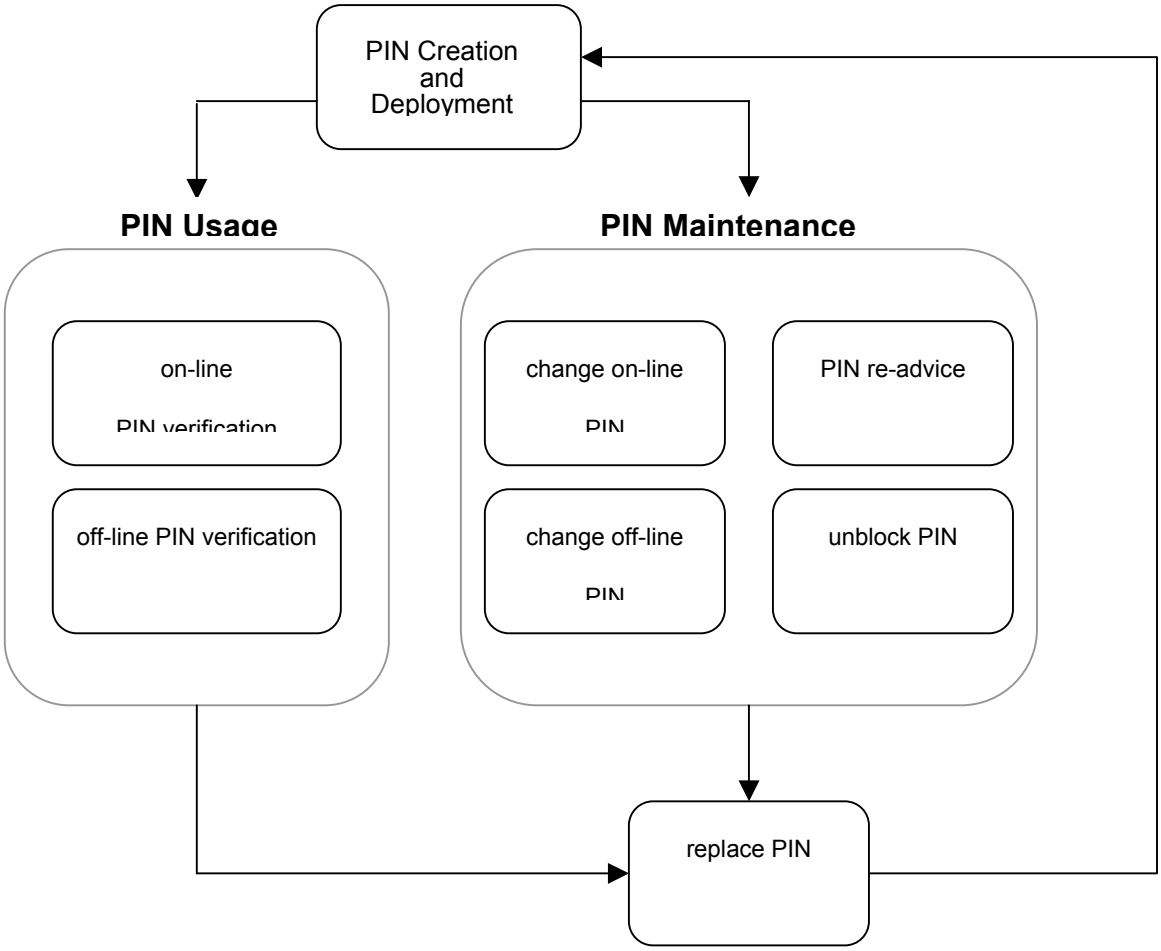


Figure 1: PIN Life Cycle

Each section in Chapters 4, 5 and 6 of this document maps to a process in this model. Note that "PIN creation and deployment" and "replace PIN" are treated as stand-alone functions; the remaining functions relate to operational PINs and are grouped as transaction functions or maintenance functions.

NOTE: The PIN unblock function is related to the PIN block condition, which is explained in 5.3 "Unblock PIN".

3 PIN Creation and Deployment

3.1 Overview

Figure 2: PIN Creation and Deployment shows the functions and security domains involved in creating PIN values, distributing them to their operational environments and advising them to customers.

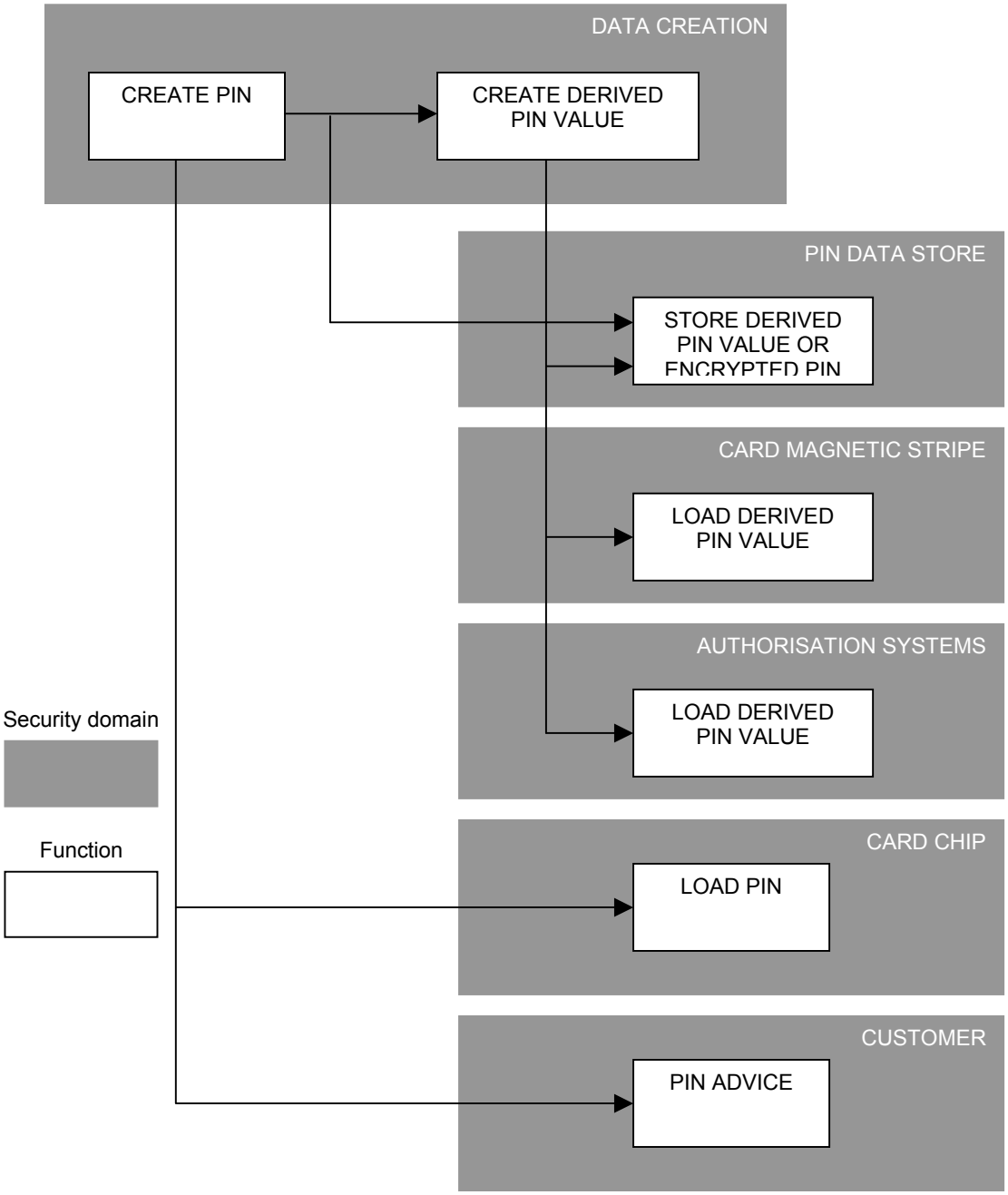


Figure 2: PIN Creation and Deployment

3.2 Create PIN

3.2.1 Context

The initial PIN value needs to be created in such a way that it is unpredictable to an outsider, and yet can be either predicted by, or distributed to, a number of parties involved in its live use. These are illustrated in "Figure 2: PIN Creation and Deployment.".

[ISO 9564] provides the following options for PIN creation:

- **Assigned derived PIN** – this involves creating the PIN in such a way that other parties can recreate the same PIN. Usually, this involves the use of a cryptographic mechanism by parties who share the same secret key.
- **Assigned random PIN** - this involves creating a PIN using a random number generation technique. This has the advantage of producing an unpredictable value, but imposes the need to construct a secure means of transporting the PIN value from the PIN creation system to the various parties that are involved in live transactions where the PIN participates.
- **Customer selected PIN** - where the customer chooses the PIN – imposes the need to construct a secure means of transporting the PIN value from the selection point to the various parties that are involved in live transactions where the PIN participates.

3.2.2 Considerations

- Cryptographic processes that support legacy PIN creation processes can introduce weaknesses. Many legacy implementations use the DES cryptographic algorithm with single strength 56 bit keys, which is now regarded as unacceptably weak.
- If random number generation processes are poorly designed, this can create weaknesses that may aid an attempt to attack the PIN creation process. For example, random number generation based on a "minutes and seconds" timestamp is inherently weak since a large range of possible numbers will never be used.
- The use of "barred" PIN values needs to be considered. In a PIN reciprocity environment customers may self-select their PINs across multiple cards issued by multiple issuers. If the industry is to deliver a common user experience then it would be inappropriate and unwelcome for each issuer to determine independently what is a valid or acceptable PIN.

3.2.3 Proposed Policy

The following policy statements are derived from [ISO 9564]

	Policy statement	Status
1	PIN creation should only be carried out: ▪ in a secure cryptographic device ▪ using an approved cryptographic algorithm and key strength (see Appendix A).	Mandatory Industry Position

2	Card issuers shall be responsible for the security of the PIN creation and deployment process except where compatibility issues arise.	Mandatory Industry Position
3	PIN lengths shall be not less 4 than numeric digits and shall not be greater than 12 numeric digits.	Mandatory Industry Position
4	The following PIN creation options shall be supported ▪ Assigned derived PIN ▪ Assigned random PIN ▪ Customer selected PIN	Mandatory Industry Position
5	A PIN should be unpredictable. The probability of guessing a PIN is approximately 1 in 10^n /t where n is the number of characters in the PIN and t is the number of PIN tries allowed. This is true for any of the PIN creation options.	Recommended
6	Card issuers should satisfy themselves as to the unpredictability of their PINs. This may be achieved either by directly testing the random qualities of PIN samples or by requiring system suppliers to demonstrate that they have done so.	Recommended
7	Where the "assigned derived PIN" option is used, the process should: ▪ Derive the PIN cryptographically from either the PAN and/or some other value associated with the customer ▪ Not contain a bias towards specific sets of values ▪ Not retain a record of the PIN, since it can be derived as required Where the PIN is derived from card data, the PIN may be used to validate that data.	Recommended
8	Where the "assigned random PIN" option is used, the process should: ▪ Create the PIN using a true random number generator, or ▪ Create the PIN using a pseudo random number generator	Recommended

9	The industry should adopt a common barred PIN list policy for use in PIN generation that is made visible and communicated to all of their customers.	Recommended
10	Multiple cards issued against a common account should each be loaded with a unique PIN created for each card.	Recommended
11	Where the "Customer selected PIN" option is used, the customer shall be provided with the necessary selection instructions and warnings. (See "Guidance to customers").	Mandatory Industry Position
12	The "Customer selected PIN" option shall be implemented to minimise the possibility that the on-line PIN and the off-line PIN are not synchronised.	Mandatory Industry Position
13	PIN selection by mail is supported **provided that**: ▪ The PIN advice form submitted by the customer identifies the account using an encrypted reference ▪ The PIN advice form does not include any other details that identify the account or customer PIN selection by mail is **not** supported if the process involves card issuer personnel handling plaintext PIN values that can be referenced to an identifiable account, since this contradicts a key security objective.	Recommended.

3.3 Store PIN

3.3.1 Context

The PIN will be stored in issuer back-end databases in order to support on-line authorisations from ATMs. It is essential that these PINs are stored securely. In the case of natural PIN values these must be stored in encrypted form. If the derived PIN Value method is used the level of security applied to protect the keys used to derive PINs must at a minimum be to the same level as given to natural PINs.

3.3.2 Considerations

- Given the attractiveness of large numbers of PINs it is essential that the physical environment is sufficiently secured, along with the appropriate personnel controls including staff vetting and dual control over all security relevant functions.
- The strength of the encryption mechanism must be sufficient for its purpose. This includes the key sizes and the key management implementation.

- There has always been considerable media attention to this element of the PIN life cycle and hence issuers should take particular care in implementing this aspect of the policy.

3.3.3 Proposed Policy

	Policy statement	Status
1	PINs must only be stored or processed: ▪ in a secure cryptographic device ▪ as enciphered data objects, using an approved cryptographic algorithm and key strength (see Appendix A), that are not identical for the same PIN value from different PANs.	Recommended
2	All aspects of the logical and physical design of the technology used in the issuers PIN storage processes, including key management implementation, and the personnel policies and procedures should be subject to regular periodic review by the issuers' internal audit function.	Recommended
3	The issuer's procedures and policies for the staff employed in PIN storage and processing operations should include pre-employment vetting of staff and during operation all security relevant operations should only be completed under dual control.	Recommended
4	At no stage should it possible for a member of staff to associate a customer's account number with his plaintext PIN value.	Recommended

3.4 Load PIN on Chip

3.4.1 Context

When the PIN has been created, it must be loaded into the chip application data. This is achieved using a proprietary manufacturer command that carries personalisation data, including the PIN value, as its data payload. EMV does not define personalisation commands.

The usual approach is for each card to support a derived card personalisation key under which the data payload is encrypted. The card personalisation key is usually calculated from a pre-loaded master key and specific card data.

3.4.2 Considerations

- If the physical environment is not sufficiently secured, this may enable an attacker to intercept and record data as they are sent to the card. This should not, in itself, be sufficient to facilitate a successful attack unless other weaknesses exist.
- The strength of the encryption mechanism must be sufficient for its purpose. This includes the key sizes and the key management implementation.

3.4.3 Proposed Policy

	Policy statement	Status
1	Between the point of PIN creation and PIN loading, PIN values shall only exist: ▪ in a secure cryptographic device ▪ as enciphered data objects, using an approved cryptographic algorithm and key strength (see Appendix A).	Recommended
2	All aspects of the logical and physical design of the technology used in the issuers end-to-end personalisation processes, including key management implementation, shall be subject to certification by card schemes.	Recommended
3	The integrity of the PIN should be protected within the card personalisation processes to ensure that the correct PIN is loaded on the correct card.	Recommended

3.5 PIN Advice

3.5.1 Context

"PIN Advice" is the process whereby PINs assigned by card issuers are advised to customers when cards are first issued. Historically, such PINs are advised to cardholders using PIN mailers. The security requirements associated with this process are well understood and documented in [ISO 9564]. Note that "PIN Advice" is distinct from the "PIN Re-advice" process, whereby forgotten PIN values are re-initialised and advised to customers. PIN Re-advice is considered in detail in 5.2 "PIN Re-advice or re-select".

3.5.2 Considerations

- The requirements in [ISO 9564] meet the needs of the UK environment.
- Alternative delivery channels utilising modern technology were considered, but were deemed to be currently insufficiently secure for PIN advice. They all may merit further consideration in the future as the security they offer matures.

3.5.3 Proposed Policy

The following policy statements are derived from [ISO 9564].

	Policy statement	Status
1	The PIN mailer shall be printed in numeric and alphanumeric characters in such a way that the plaintext PIN cannot be observed until the envelope is opened.	Recommended.
2	The envelope shall display the minimum data necessary to deliver the PIN mailer to the correct customer.	Recommended.
3	A PIN mailer shall be constructed in such a way that it is highly likely that accidental or fraudulent opening will be obvious to the customer.	Recommended.
4	The card issuer shall warn the customer not to use a PIN that is contained in an opened or tampered PIN mailer and to notify the card issuer of such an event. (See also "Guidance to customers").	Recommended.
5	The PIN and the card should not be mailed in the same mailer, nor at the same time.	Recommended.
6	At no point in the delivery process shall the PIN appear in plaintext where it can be associated with a customer's account.	Recommended.

3.6 On-line PIN checking mechanisms

3.6.1 Context

The three on-line PIN checking mechanisms in common use are PIN reference Values, PIN offset and PVV. Because of the historical evolution of these methods, the terminology is sometimes misused – in particular, PIN offset is often used to describe a PVV implementation.

The three methods may briefly be described as follows:

PIN Reference Values	This uses an enciphered reference PIN block bound with the card PAN cryptographically, and optionally other cardholder based data e.g. cardholder identity and PIN Issue number. The cryptogram is reversible to ensure that only one PIN value can be legitimately mapped to one cardholder at any given time. It enables randomly created PIN values to be maintained independent of a PIN Generation Key, avoids the use of any decimalisation tables and supports the flexibility of changing the PAN on renewal.
PIN offset	The PIN offset method was originally deployed to support first generation ATMs used in the offline mode. It relies upon a base PIN being derived cryptographically from the customer's PAN, and then

	by the modulo-10 addition of an offset the final PIN is created that the customer will use. In these early off-line ATMs the cryptographic key, offset and customer PIN and PAN would have been used to verify the customer. More normally now the PIN offset value is stored in the issuer's host systems and is used in an online ATM authorisation system, whilst also providing the capability for the customer to self-select his PIN and this is reflected in a new offset value on the host system.
PVV	The PIN Verification Value (PVV) is specified by Visa. The PIN and the card data are combined and encrypted using the Triple DES algorithm with a double length key. The result is converted to 4 decimal digits. Note that this is a one-way function and that it is possible for more than one PIN value to satisfy the PVV check.

The PIN offset or the PVV may be recorded on the magnetic stripe, whilst the PIN reference value is never placed on the magnetic stripe nor distributed to stand in processors. The on-line protocol between the ATM device and the issuer systems include the transaction PIN keyed by the customer and the PIN offset or PVV on the magnetic stripe.

In the case of a PIN offset check, the issuer systems use the card data and transaction PIN to recompute the PIN offset, which is then compared to the PIN offset reference value.

In the case of a PVV check, the transaction PIN is subjected to the PVV one-way process and the result is compared with the PVV reference value.

3.6.2 Considerations

- Historically, many PIN offset implementations were designed using the single DES algorithm and may continue to do so. The strength of some legacy PIN offset calculations may therefore no longer be adequate to prevent exhaustive search attacks.
- The design of some PIN offset calculation mechanisms may produce PIN offset values which are inadequately diversified and may be vulnerable to collision based attacks.

3.6.3 Proposed Policy

	Policy statement	Status
1	PIN offset values, where used, shall use cryptographic mechanisms that conform to the requirements in Appendix A.	Mandatory Industry Position

4 PIN Usage

4.1 On-Line PIN verification

4.1.1 Context

On-line PIN verification is the process that compares the transaction PIN (the value keyed by the cardholder, or a derived version) with the on-line reference PIN (the value known to the card issuer, or a similarly derived version). In UK this will only be done within ATM environments and not in the point-of-sale environment.

The process involves the use of functions handling encrypted PIN blocks across multiple security domains, as illustrated in Figure 3.

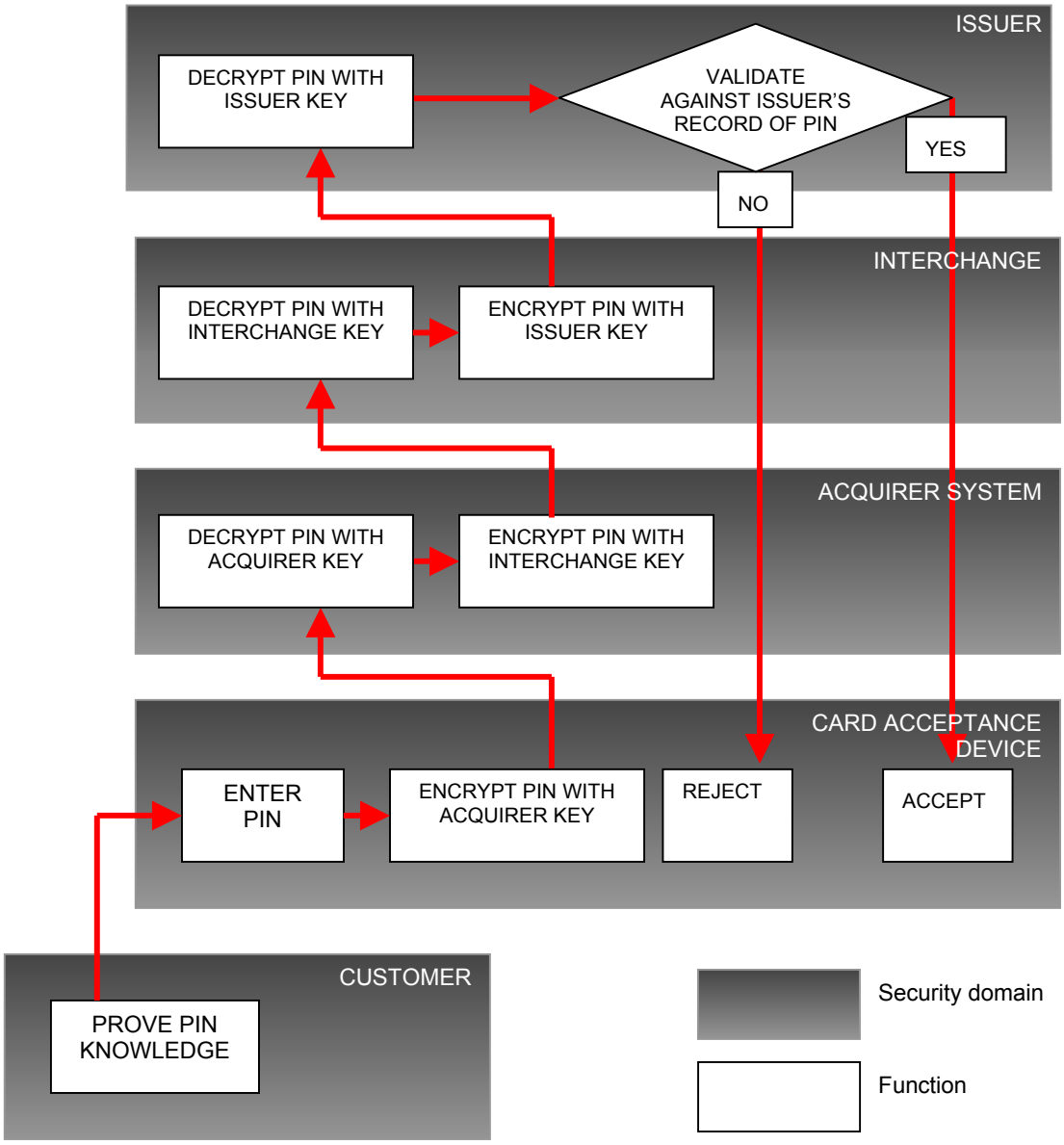


Figure 3: On-line PIN Verification

This example has been simplified to illustrate the process of moving the transaction PIN across successive security domains. For example, on-line PIN verification may use an on-line reference PIN, a PIN offset or a PVV. In the case of an on-line reference PIN, the sequence of events is:

1. The customer keys the transaction PIN into the card acceptance device.
2. The card acceptance device creates a PIN Block data object, following an industry standard format. This includes the transaction PIN. The PIN Block is encrypted using an "Acquirer Key"- a symmetric cryptographic key that is shared with the acquirer host system.
3. The acquirer host system uses the Acquirer Key to recover the plaintext PIN Block. This is re-encrypted using the "Interchange Key" a symmetric cryptographic key that is shared with the interchange network.
4. The interchange network uses the Interchange Key to recover the plaintext PIN Block. This is re-encrypted using the "Issuer Key" a symmetric cryptographic key that is shared with the interchange network. The interchange network routes the re-encrypted PIN Block to the card issuer system.
5. The card issuer system uses the Issuer Key to recover the plaintext PIN Block. The transaction PIN is matched to a reference PIN stored in a card issuer database.
6. If the two values match, the transaction is authorised and an authorisation message is sent to the card acceptance device.

4.1.2 Considerations

- The LINK Security Standard provides the baseline security requirements for PIN protection within the UK's ATM interchange environment.
- If incorrectly designed, PIN Block formats may create interoperability problems and may facilitate some types of replay or cryptanalysis attacks.
- Where legacy encryption processes are not up to date, there is the risk that encrypted messages could be attacked, leading to compromise of PIN values. The following specific risks are relevant:
    - The single strength DES encryption algorithm is widely implemented. This is no longer considered to provide adequate protection. (see APPENDIX A – Approved cryptographic mechanisms).
    - The quality of key management constitutes a risk if improperly implemented.
    - The physical and logical security that protects the cryptographic environment constitutes a risk if improperly implemented.
- If unauthorised access to the reference PIN database occurs, there is the risk that PIN values could be compromised.
- If unprotected, there exists the risk that the issuer authorisation message could be intercepted and either modified, or replayed, to fool the card acceptance device into authorising transactions.

4.1.3 Proposed Policy

These policy statements should be read in conjunction with those under 3.3.3

	Policy statement	Status
1	PIN Block formats shall be interoperable and shall conform to [ISO_9564].	Mandatory Industry Position
2	The strength of encryption mechanisms shall be sufficient to minimise the risk of security breaches through exhaustive key search or through cryptanalysis. Cryptographic algorithms and key strength lower bounds shall conform to the requirements in Appendix A.	Mandatory Industry Position
3	Cryptographic keys shall be managed in a way which minimises the risk of key compromise. The following principles shall be observed: ▪ Key management procedures shall conform to the ISO 11568 standard and with scheme rules. ▪ Keys shall be distributed either under the protection of key encryption keys or techniques based on split knowledge and multiple control. Keys shall not be used for more than one purpose. Keys shall be replaced periodically. In the event of compromise, a key shall be replaced immediately.	Mandatory Industry Position
4	Cryptographic functions shall be executed in secure cryptographic devices that comply, as a minimum, to the level 3 standard in [FIPS_140], or equivalent.	Mandatory Industry Position
5	The validation process in which the PIN offered by the customer and the reference PIN should only be completed within a hardware security module.	Recommended
6	Reference PIN databases shall be secured to protect the integrity and confidentiality of reference PINs.	Mandatory Industry Position
7	Only encrypted PIN values should be stored in the reference database.	Recommended
8	The integrity of card issuers' authorisation messages should be protected to minimise the risk of replay or modification attacks.	Recommended

4.2 Off-line PIN verification

4.2.1 Context

Off-line PIN verification is the process that compares the transaction PIN (the value keyed by the cardholder) with the off-line reference PIN (the value stored in the chip). This involves moving the keyed PIN across three security domains as illustrated in Figure 4 below:

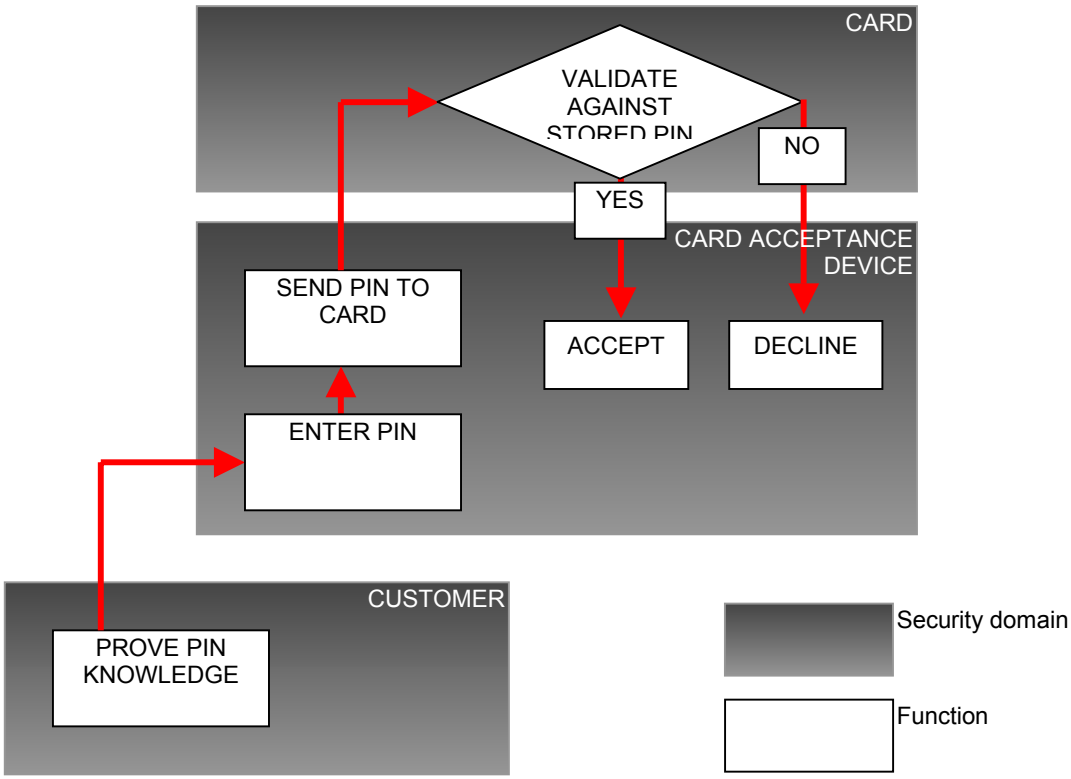


Figure 4: Off-line PIN security domains

The EMV specification provides two options for implementing this process:

- Cards which support the Dynamic Data Authentication function will be able to use public key cryptography to import the transaction PIN in encrypted form. The card then uses its private key to recover the plaintext transaction PIN and compare it to the reference PIN stored in the card.
- Cards which support the Static Data Authentication function will only be able to import the transaction PIN in unencrypted form. This is then compared directly with the reference PIN stored in the card.

Where the transaction PIN and the reference PIN match, off-line PIN verification is successful and the card returns a "success" response code.

4.2.2 Issues

The following issues need to be addressed:

- If the PIN is inadequately protected when handled by the card acceptance device, the confidentiality of the PIN is at risk.

- There exists the risk of counterfeit cards that are programmed to replay genuine card data and Static Data Authentication signatures skimmed from genuine cards. In such cases, off-line PIN verification cannot be relied upon. The counterfeit card will only be detected if the transaction is processed on-line.

4.2.3 Proposed Policy

	Policy statement	Status
1	Card acceptance devices shall use the card public key to protect transaction PINs where such a key is available.	Mandatory Industry Position
2	Card acceptance devices shall incorporate tamper-responsive measures to protect against intrusive attacks	Mandatory Industry Position
3	PIN Entry Devices (PEDs) shall be evaluated to EAL4+ under the Common Criteria Evaluation Methodology; the security requirements that PEDs shall meet in this evaluation are expressed in the PED Protection Profile [PED].	Mandatory Industry Position

5 PIN Maintenance

5.1 Change PIN

5.1.1 Context

It is industry policy for all customers to be offered the option to self-select PIN values and for the separate off-line and on-line PIN values to be transparent to customers. This means that, where the customer selects a new PIN, both the on-line off-line PIN values must be changed.

Changing the on-line PIN involves changing the reference PIN known to the card issuer, which requires an on-line session with the card issuer. [ISO 9564] provides current industry standards for changing on-line PINs.

Changing the off-line PIN involves using the PIN CHANGE/UNBLOCK command, which carries the PIN value as its data payload and requires the presence of a MAC to authenticate that payload. This means that this process can only be changed at an ATM in an on-line session with the card issuing system.

5.1.2 Considerations

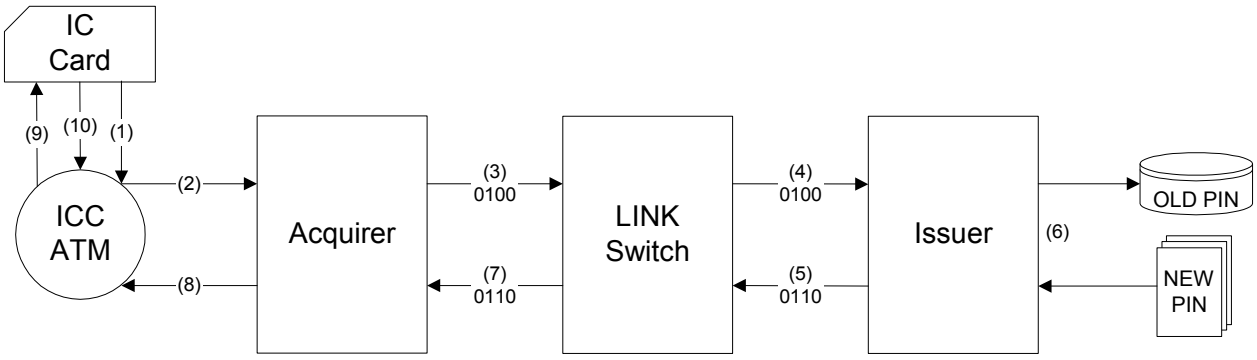
A consequence of adopting PIN @ POS in the UK with our differentiated market of card products will be the demand for customers to align their PINs across the multiple cards that they own from multiple issuers. The Financial Ombudsman Service (formerly the Banking Ombudsman) explicitly supports this demand. The major technical considerations in order to allow this facility are:

- The processes needed to synchronise on-line PIN changes with off-line PIN changes.
- The method of synchronising PIN changes should provide a consistent experience from the customer viewpoint.
- To consider the need for PIN changes to be suppressed during the period immediately prior to card renewal, when the renewed PIN might otherwise be out of line with the newly selected PIN.

5.1.3 LINK PIN Management Service for Reciprocal PIN Change

Figure 5 provides a high level example of how the protocol has been designed. It addresses the following requirements:

- effects a synchronous change of both the on-line and the off-line PIN; and
- preserves, as far as possible, service to the customer by reverting to the original PIN in the event that the full protocol fails to complete.



(1)/(2) Represents the message flows between the card, ATM and the acquirer host which result in the old PIN block and the single new PIN block being available to be sent to LINK. Note that the two entries of the new PIN have already been compared to ensure that they are the same.

(3) is the authorisation request containing both the old and new PIN blocks from the acquirer to LINK.

(4) is the authorisation request containing both the old and new PIN blocks from LINK to the issuer. The issuer checks that both the old and new PINs are valid.

(5) is the approval response to LINK containing the issuer script to change the off-line PIN on the card.

(6) The new on-line PIN is changed by the issuer, and the old on-line PIN is stored in case of a PIN Management Failure message is received. This is at the issuer's discretion.

(7) is the approval response to the acquirer from LINK containing the issuer script.

(8) is the approval response to the ATM from the acquirer host.

(9) represents the updating of the off-line PIN on the card.

(10) is the response from the card saying that the off-line PIN change was successful. At this point, the customer is shown a screen to the effect that the PIN change has been successful.

Figure 5: LINK PIN Management Service

This protocol is designed for interchange environment but may also valid for "on us" transactions. In the case of PIN changes across the interchange environment, the method of PIN Block encryption will be the same as that described in section 4.1 above.

It should also be noted that, in the case of "on us" transactions, the PIN Change protocol may need to co-exist with an "Unblock PIN" protocol. Again, for simplicity, this is not shown in Figure 5.

5.1.4 PIN Change using the Issuer's Public Key

It is recognised that there are potential weaknesses associated with the design of a PIN Change protocol in an interchange environment. These mainly relate to the need for separate PIN blocks containing the reference PIN and the newly selected PIN values. It is possible to theorise attacks that intercept and modify such components. Such concerns increase in the international interchange environment.

These concerns can be overcome if the PIN Block components can be protected using the issuer public key. This removes the dependence on acquirer and interchange keys. A

proposal has been submitted to modify the draft DIS 9564-1 standard to permit reciprocity to be designed in this way. Any new standards that emerge for PIN change will be incorporated in this document under normal change management procedures.

5.1.5 Proposed Policy

The proposed policy statements detailed below are based on the requirements in [ISO 9564], and also they should be read in the context of those policy statements at 3.2.3 and 3.3.3.

	Policy statement	**Status**
1	On-line PIN change should be supported through an ATM, or secure unattended devices at a card issuer's location. The procedure shall require the current PIN to be entered and verified before selection and activation of the new PIN. The new PIN shall be entered twice and the terminal shall ensure that both entries are identical.	Recommended
2	On-line PIN change may be supported through an attended terminal at a card issuer location.	Recommended

The following are additional policy statements based on the business requirements of the PIN @ POS Programme.

3	In all cases where an ATM supports on-line PIN change, it shall support off-line PIN change, and this must be effected in the same transaction. The transaction protocol must ensure that the on-line and off-line PINs are always aligned. Thus, any failures, such as "time-outs" shall result in a "roll-back" to the original PIN value.	Mandatory Industry Position.
4	An industry protocol to support synchronous changes to on-line and off-line PINs across the interchange environment should be defined. Section 6.1.3 demonstrates an example of such a protocol design.	Recommended
5	The PIN change protocol shall support synchronisation by recognising exception conditions such as time-outs. Thus, unless the protocol demonstrates that both the on-line and the off-line PINs have been changed successfully, the PIN values must roll back (where possible) to the original PIN value.	Mandatory Industry Position
6	Where an on-line PIN update has been completed, but the off-line PIN update cannot be completed due to a system fault (between steps 5 and 6) there is the risk that	Recommended

	the on-line and off-line PIN values cannot not be synchronised. Card Issuers should recognise such a condition either by receiving a failure message in step 6 or by the non-receipt of this message. Card issuers should implement procedures to identify such a condition when it occurs and to display appropriate instructions to the cardholder.	
7	A PIN Change event should be recorded for future dispute resolution. This record should not include any plaintext PIN values.	Recommended
8	The industry should adopt the policy that when customers self-select a PIN none of their choices should be barred. Customers should however be provided with advice regarding how to choose a secure PIN.	Recommended

5.2 PIN re-advice or re-select

5.2.1 Context

It is a business requirement for card issuers to provide support to customers who have forgotten their PINs.

The options for dealing with forgotten PINs are:

- **Full Card and PIN replacement**: this is the option that can most reliably be secured and is, therefore, historically the preferred approach.
- **PIN re-advice**: this option most readily meets card issuers' business requirements since, in many cases, it can be implemented immediately through various channels and does not require a session to write new data to the chip. It must be assumed that there will be a proportion of cases where the existing (forgotten) off-line PIN has become blocked and, in these cases, an on-line session will be required to unblock the PIN. In all cases, PIN re-advice is extremely difficult to implement securely because of the need to authenticate the customer and to protect the confidentiality of the PIN during the re-advice process; therefore from a security perspective it is recommended that a PIN re-advice should be conducted wherever possible as a PIN replacement exercise.
- **PIN re-select**: this option effectively involves a customer authentication followed by a "PIN Change" as previously described. It may therefore be executed more rapidly than a card and PIN replacement, but must be performed in devices that support active data sessions with the chip and on-line sessions with card issuer systems.

5.2.2 Considerations

- Issuers need to determine their solution for their customers; PIN re-advice, or PIN re-select, or both.
- The considerations for a range of PIN advice channels, with associated risks, are described earlier in this document.

- The only recommended option for PIN re-select is through bank-attended devices.

5.2.3 Proposed Policy

	Policy statement	Status
1	PIN re-advice may be implemented, at the card issuer's discretion, through the following channel: ▪ Tamper-evident mail The use of IVR systems is **not** supported. In all cases, the policies described in 3.5 "PIN Advice" apply.	Recommended
2	PIN re-select should only be implemented through a card issuer's attended devices.	Recommended
3	A card issuer may enter into individual PIN change reciprocity arrangements with other parties.	Recommended

5.3 Unblock PIN

5.3.1 Context

To prevent exhaustive attempts to determine an offline PIN value, the Chip Application blocks the PIN after a predetermined number of incorrect PINs (known as the PIN Try Limit). Each incorrect PIN value causes the PIN Try Counter to be decremented by 1. When the value of the PIN Try Counter reaches 0, the Chip Application blocks the offline PIN.

The PIN may be unblocked by setting the PIN Try Counter (PTC) to the PIN Try Limit (PTL) by using the PIN CHANGE/UNBLOCK command. The current risk profile under the PIN @ POS programme has determined that this command should only be undertaken at ATMs.

This command incorporates a MAC calculated by the card issuer. The card issuer and the card share a MAC master key - this, along with the Chip transaction counter, is used to create a session key which computes the MAC. Upon successful completion of the PIN CHANGE/UNBLOCK command, the PIN is unblocked and the PIN Try Counter is reset to the PIN Try Limit.

Any PIN Unblock implementation therefore requires a real-time data interchange session with the card issuer.

5.3.2 Consideration

Issuers will need to determine their criteria for authenticating customers prior to allowing PIN Unblock.

5.3.3 Proposed Policy

	Policy statement	Status
1	ATMs shall support Issuer Script Messaging and the PIN CHANGE/UNBLOCK command.	Mandatory Industry Position
2	Where a PIN-blocked card has successfully completed an on-line PIN verification at an ATM, card Issuers should execute the PIN Unblock function.	Recommended
3	Card Issuers may choose to implement additional or alternative security measures before executing the PIN Unblock function through an ATM, in which case the ATM display should advise cardholders to contact the card issuer.	Recommended
4	Cardholders shall be offered clear guidance on the procedure for unblocking the PIN.	Mandatory Industry Position
5	Cardholders shall be informed at the ATM whether PIN Unblock has been successfully applied.	Mandatory Industry Position
6	Unblock PIN shall not be supported in the POS network.	Mandatory Industry Position

6 Guidance to customers

It is recommended that guidance material issued to customers should include the following advice. These recommendations are derived from [ISO 9564].

6.1 General safekeeping

1. Customers should be advised to contact the card issuing institution if the PIN mailer is not received or has not been received intact.
2. Customers should be advised to memorise the PIN and never to write it down. The PIN mailer should be destroyed.
3. Customers should be advised never to orally communicate the plaintext of a PIN to any person or device.
4. Customers should be made aware that no procedures exist which would ever require them to disclose their PIN value to any person purporting to be bank, retailer or police personnel.
5. Customers should be advised to contact their card issuer immediately if they suspect that their PIN has been compromised.

6.2 Selecting and changing PINs

(see 5.1 “Change PIN”)

1. When the customer selects or changes a PIN, they should be advised of the following:
   - That the selected PIN should not be a value that is readily associated with the customer.
   - That the selected PIN value should not comprise an easily guessed number; examples of easily guessable numbers includes:
     - A sequence from the associated account number;
     - Strings of the same number; and
     - Obviously significant dates (such as birthdays and anniversaries).
2. When a customer-initiated PIN change is put into effect, a notification of the change, but not the value, should be mailed to the customer. The notification should include instructions to contact the issuer immediately if the customer had not requested the change.

6.3 PIN usage

1. Customers should be advised to enter PINs in a way that cannot be observed or noted by others.

APPENDIX A – Approved cryptographic mechanisms

Symmetric Block Cipher algorithms

Algorithm	Key strength lower bound	References
Triple DES	112 bits	X9.52 (98) – this specifies the use of Triple DES and replaces the earlier FIPS standards. The use of single strength (56 bit) DES is no longer supported in Federal Standards; the APACS position requires it to be discontinued in the UK from 2005. MasterCard and VISA have each mandated that for any of their transactions, host to host messages must have their PIN block triple DES encrypted by April and December 2003 (respectively) and that all ATMs and devices must use triple DES by April and December 2005 (respectively).

Symmetric Block Cipher implementation modes

Implementation	Key strength lower bound	Remarks
Cipher-block chaining mode (CBC)	112 bits	
Cipher feedback mode	112 bits	
Output feedback mode (OFB)	112 bits	
Derived Unique Key Per Transaction (DUKPT)	112 bits	

Public Key Algorithms

Algorithm	Key strength lower bound	References
RSA	Next replacement key length published by card schemes	ANSI X9.31-1